What is claimed is:

1. A system employed by a first application for encoding URL link data for use in detecting unauthorized URL modification, comprising:

an input processor for receiving an encryption key;

a URL processor for processing a URL link to a second application using said received encryption key by identifying URL type and adaptively encrypting a URL link address portion based on said identified type to produce a processed URL; and

a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

2. A system according to claim 1, wherein

said encryption key is received from a managing application responsible for providing said encryption key to a plurality of concurrently operating applications.

3. A system according to claim 1, wherein

said communication processor communicates said URL link address portion to a managing application for encryption.

4. A system according to claim 1, wherein

said URL processor of said first application adaptively processes a URL link to a second application differently to a link to a web page provided by said first application.

5. A system according to claim 4, wherein

said URL link to a second application includes an encrypted address portion and said link to said web page provided by said first application includes a non-encrypted address portion.

6. A system according to claim 1, including

a browser application for providing a user interface display permitting user entry of identification information and for providing user identification information to said first application wherein

said first application authenticates said user identification information prior to permitting user access to functions of said first application.

7. A system according to claim 1, wherein

said URL processor compresses said URL link address portion and encrypts a compressed URL link address portion.

8. A system according to claim 7, wherein

said URL processor compresses said URL link address portion using a hash function.

9. A system according to claim 7, wherein

said communication processor communicates said URL link address portion to a managing application for compression.

10. A system according to claim 1, wherein

said URL processor adaptively generates URL fields including an encrypted URL address portion and a non-encrypted session identifier; and

11. A system for encoding URL link data for use in detecting unauthorized URL modification occurring during concurrent operation of a plurality of applications, comprising:

a managing application for providing a common encryption key to a plurality of concurrently operating applications; and

a first application including,

an input processor for receiving said encryption key;

a URL processor for processing a URL link to a second application using said received encryption key by identifying URL type and adaptively encrypting a URL link address portion based on said identified type to produce a processed URL; and

a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

12. A system according to claim 11, wherein

said communication processor communicates said URL link address portion to said managing application for encryption.

13. A system according to claim 11, wherein

said URL processor compresses said URL link address portion and encrypts a compressed URL link address portion.

14. A system according to claim 13, wherein

said URL processor compresses said URL link address portion using a hash function.

15. A system according to claim 13, wherein

said communication processor communicates said URL link address portion to said managing application for compression.

16. A system for encoding URL link data for use in detecting unauthorized URL modification, comprising:

a browser application for providing a user interface display permitting user entry of identification information for providing user identification information to a first application;

a first application responsive to said user identification information including,

a URL processor for adaptively generating URL fields including an encrypted URL address portion for incorporation together with a non-encrypted portion in a processed URL; and

a communication processor for including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

17. A system according to claim 16, wherein

said communication processor communicates said URL address portion to another application for encryption.

18. A system for processing URL link data for detecting unauthorized URL modification and suitable for use by a plurality of concurrently operating applications, comprising:

a first application including,

a URL processor for adaptively generating a URL link to a second application differently to a URL link to a web page provided by said first application, to provide a generated URL; and

a communication processor for including said generated URL in data representing a web page and for communicating said web page representative data including said generated URL to a requesting application.

19. A system according to claim 18, wherein

said URL processor,

(a) generates a URL field including an encrypted URL address portion for incorporation together with a non-encrypted URL portion in said generated URL link to said second application, and

(b) provides a URL including a non-encrypted URL address portion in said generated URL link to said web page provided by said first application.

20. A system supporting concurrent operation of a plurality of Internet compatible applications, comprising:

a browser application including,

a display generator for providing a user interface display permitting user entry of identification information and commands for a plurality of Internet compatible applications and for providing user identification information to a first application;

a URL generator for adaptively generating a URL including URL fields incorporating an encrypted URL address portion and a non-encrypted session identifier; and

a processor for initiating communication of said generated URL to said first application in response to validation of said user identification information.

21. A method employed by a first application for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications, comprising the steps of:

receiving an encryption key;

processing a URL link to a second application using said received encryption key by identifying URL type and adaptively encrypting a URL link address portion based on said identified type to produce a processed URL; and

including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

22. A method employed by a first application operating in a system supporting concurrent operation of a plurality of Internet compatible applications, said method comprising the steps of:

in response to a command from a request device to initiate a first application,

enabling user operability of said first application based upon validation of user identification information;

encrypting a link to a second application;

including said encrypted link in data representing a web page to be returned to said request device; and

communicating to said request device, said web page representative data including said encrypted link.

23. A method for encoding URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications, comprising the steps of:

providing a common encryption key to said plurality of concurrently operating applications; and

receiving said encryption key;

processing a URL link to a second application using said received encryption key by identifying URL type and adaptively encrypting a URL link address portion based on said identified type to produce a processed URL; and

including said processed URL in data representing a web page and for communicating said web page representative data including said processed URL to a requesting application.

24. A method for processing URL link data for use in detecting unauthorized URL modification in a system supporting concurrent operation of a plurality of applications, comprising the steps of:

adaptively generating a URL link to a second application differently to a URL link to a web page provided by said first application, to provide a generated URL; and

including said generated URL in data representing a web page and for communicating said web page representative data including said generated URL to a requesting application.